



RECEIVED
OCT 24 2003
Technology Center 2100

ATTACHMENT A

The claims:

Cancel ~~claims 1-47~~ of the application as originally filed and add the following new claims 48-85.

1-47 (canceled)

48. (new) A method for a person to sign a hard copy or a digital document by use of a signature sensing device, including the steps:

- 5 (a) capturing a capturable signature of the person using the sensing device;
- (b) generating a verification ID; and
- (c) attaching the capturable signature, the verification ID and an optical
- A₁ watermark to the document to complete the document signing process,

characterized in that

the capturable signature is embedded into the optical watermark, and the verification ID is generated from one or more of the group consisting of: the capturable signature, a document digest, representative features of the document, and a time stamp.

49. (new) A method as claimed in claim 48, characterized in that one or more selected from the group consisting of: the document digest and a time stamp, is embedded into the optical watermark to form a link between the document and the capturable

20 signature; the document digest being critical information of the document.

50. (new) A method as claimed in claim 48, characterized in that the person's identity is verified by a public key infrastructure after a security handshaking challenge-and-response session between a server and the sensing device; the sensing device storing

25 one or more selected from the group consisting of: an identity number of the sensing device, a private key of the sensing device, a private key of the person, measured features of the person's capturable signature, and a detachable learning module.

51.(new) A method as claimed in claim 50, characterized in that there is a plurality of persons able to use the sensing device, the sensing device being able to store registration information of each such person.

5 52. (new) A method as claimed in claim 51, characterized in that the server and sensing device store their private keys respectively, and the capturable signature and/or measured features of the capturable signature of the person are stored in the server; there being included a preliminary step of security handshaking between the server and the sensing device based on public key pairs.

A. 10 53. (new) A method as claimed in claim 52, characterized in that the capturable signature and/or measured features of the capturable signature of the person are stored in the sensing device, and the processing and verification of the capturable signature are also carried out inside the sensing device.

15 54. (new) The method as claimed in claim 53, characterized in that there is a security authentication process between the server and the sensing device, as well as between the server and a service program; and after successful completion of the security handshaking, the sensing device collects capturable signature data, encrypts the capturable signature data, and sends it to the server for further processing and verification.

55. (new) A method as claimed in claim 54, characterized in that the capturing and processing of the capturable signature and/or measured features of the capturable
25 signature of the person are carried out in a secure processor; the processing result being sent to the sensing device for verification.

56. (new) A method as claimed in claim 55, characterized in that the private key and the capturable signature of the person are stored in the sensing device.

57. (new) A method as claimed in claim 55 characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in the secure processor.

58. (new) A method as claimed in claim 55, characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in the server.

59. (new) A method as claimed in claim 55, characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in an encrypted form.

60. (new) A method as claimed in claim 55, characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in a secure memory.

61. (new) A method as claimed in claim 60, characterized in that the secure memory is an authentication card for the person.

62. (new) A method as claimed in claim 55, further including a document-handling module in the computer for displaying the document and incorporating the capturable signature into the document.

63. (new) A method as claimed in claim 62, further including at least one seal image in the sensing device so that upon signing the document both the capturable signature of the person and the at least one seal image will appear on the document.

64. (new) A method as claimed in claim 63, characterized in that the at least one seal image is the optical watermark in which is embeded hidden information to protect against forgeries

5 65. (new) A method of claim 64, characterized in that the method is applied to process approval.

66. (new) A method for generating a validated capturable signature to a document including the steps of:

- 10 (a) signing the document using signature sensing device;
(b)creating a digest of the document;
(c) encrypting the capturable signature within the sensing device;
(d)generating a verification ID; and
(e) attaching the capturable signature and the verification ID and an optical
15 watermark to the document to complete the document signing process, characterized in that one or more selected from the group consisting of: the capturable signature, the document digest, and critical features of the document, are embedded into the optical watermark to form a link between the document and the capturable signature.

20 67.(new) A method as claimed in claim 66, characterized in that the verification ID is generated from one or more of the group consisting of: the capturable signature, the document digest, representative features of the document, and time stamp.

25 68. (new) A method as claimed in claim 67, characterized in that the capturable signature and the time stamp are encrypted using an encryption key, the encryption key being generated from the document digest.

69. (new) A method as claimed in claim 68, characterized in that the encryption key is generated by using the document digest to query an encryption key pair from an encryption key database in one of: the sensing device, a server, or a secure memory.

5 70. (new) A method as claimed in claim 68, characterized in that the encryption key is generated by using the document digest as a seed to generate an encryption key pair inside one selected from the group consisting of: the sensing device, a server, and a secure memory,

and using a secret function stored in one of: the sensing device, the server, and the secure memory.

A₁
71. (new) A method as claimed in claim 68, characterized in that the digest of the document is obtained from the representative features of the document.

15 72. (new) A method as claimed in claim 71, characterized in that the capturable signature is extracted from a printed form of the document when the document to be verified is a printed document.

73.(new) A method as claimed in claim 68, characterized in that the encryption key is
20 one of a public key pair and a symmetry key.

74. (new) A method as claimed in claim 64, characterized in that the capturable signature includes signature image and features of the capturable signature when features of the capturable signature are captured; the features of the capturable
25 signature captured including pressure and speed.

75. (new) A method as claimed in claim 71, characterized in that the capturable signature includes signature image and features of the capturable signature when features of the capturable signature are captured; the features of the capturable
30 signature captured including pressure and speed.

76. (new) A method as claimed in claim 50, characterized in that pre-registered capturable signatures are stored for future use in one or more selected from the group consisting of: the sensing device, the server, and a secure memory.

5

77. (new) A method as claimed in claim 68, characterized in that pre-registered capturable signatures are stored for future use in one or more selected from the group consisting of: the sensing device, the server, and a secure memory.

10 A1 78. (new) A method as claimed in claim 64, characterized in that the capturable signature is combined other with biometric information of the person.

79. (new) A method as claimed in claim 72, characterized in that the capturable signature is combined other with biometric information of the person.

15

80. (new) A method as claimed in claim 64, characterized in that the authenticity of the signed document is verified by:

- (a) creating a digest of the signed document;
- (b) querying or generating a decrypt key using the document digest, and decrypting the verification ID; and
- (c) verifying the validity of the capturable signature by comparing the capturable signature extracted from the verification ID and the capturable signature as it appears on the signed document.

25 81. (new) A method as claimed in claim 72, characterized in that the authenticity of the signed document is verified by:

- (d) creating a digest of the signed document;
- (e) querying or generating a decrypt key using the document digest, and decrypting the verification ID; and

(f) verifying the validity of the capturable signature by comparing the capturable signature extracted from the verification ID and the capturable signature as it appears on the signed document.

82. (new) A method as claimed in claim 80, characterized in that there is included the additional step of verifying the authenticity of the document by comparing the document digest and a digest from the verification ID.

A1
Cond.

83. (new) A method as claimed in claim 81, characterized in that there is included the additional step of verifying the authenticity of the document by comparing the document digest and a digest from the verification ID.

84. (new) A method as claimed in claim 82, characterized in that there is included the further step of verifying the authenticity of the document by comparing the capturable signature on the document and critical features of the document with that embedded in the optical watermark.

85. (new) A method as claimed in claim 83, characterized in that there is included the further step of verifying the authenticity of the document by comparing the capturable signature on the document and critical features of the document with that embedded in the optical watermark.
